

AMENDMENTS TO THE CLAIMS

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 were pending at the time of the Action.

Claims 1, 10, 12, 16, 24, 26, 31, 38, 40, 49, and 58 are amended.

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 remain pending.

1. (Currently Amended) A method for constraining a scope of delegation by a client to a server, comprising:

identifying a target service to which access is sought on behalf of a client;

causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third-party, wherein the server provides the trusted third-party with a credential authenticating the server, information about the target service, and a service credential previously provided by the client to the server; and

causing the trusted third-party to provide the server with a new service credential granted in the name of the client rather than the server such that the new service credential authorizes the server to access the target service on behalf of the client while withholding a client's authentication credentials from the server, wherein the new service credential granted in the name of the client is constrained to a scope specified by the service credential previously provided by the client to the server.

1           2.     (Original)   The method as recited in Claim 1, wherein the  
2 trusted third-party includes at least one service selected from a group of  
3 services comprising a key distribution center (KDC) service, a certificate  
4 granting authority service, and a domain controller service.

5  
6           3.     (Canceled).

7  
8           4.     (Previously Presented) The method as recited in Claim 1,  
9 wherein the new service credential is configured for use by the server and the  
10 target service to which access is sought.

11  
12           5.     (Previously Presented) The method as recited in Claim 1,  
13 wherein the credential authenticating the server is a ticket that includes a ticket  
14 granting ticket associated with the server.

15  
16           6.     (Original)   The method as recited in Claim 1, further  
17 comprising:

18               causing the trusted third-party to verify that the client has authorized  
19 delegation.

20  
21           7.     (Original)   The method as recited in Claim 6, wherein:  
22 the trusted third-party includes a key distribution center (KDC); and  
23 causing the trusted third-party to verify that the client has authorized  
24 delegation includes verifying the status of a restriction placed on the ticket  
25 originating from the client.

1           8.     (Original)   The method as recited in Claim 1, further  
2 comprising:

3           causing the trusted-third-party to selectively determine if the client is  
4 allowed to participate in delegation either based on information selected from a  
5 group comprising an identity of the client, a group affiliation associated with  
6 the client.

7  
8           9.     (Original)   The method as recited in Claim 1, wherein the  
9 server is a front-end server with respect to a back-end server that is coupled to  
10 the front-end server, and wherein the back-end server is configured to provide  
11 the target service to which access is sought.

12  
13           10.    (Currently Amended)   The method as recited in Claim 1,  
14 wherein:

15           the trusted third-party includes a key distribution center (KDC);

16           the KDC provides the client's authentication credentials as a ticket-  
17 granting-ticket associated with the client to the client; and

18           the client does not provide the ticket granting ticket to the server.

19  
20           11.    (Original)   The method as recited in Claim 1, wherein:

21           the trusted third-party includes a key distribution center (KDC); and

22           the server requests the new credential in a ticket granting service request  
23 message that includes a service ticket provided by the client to the server.

1           12.   (Currently Amended)   A method for constraining the scope of  
2   authentication credential delegation by a client to a server, comprising:

3           identifying a target service to which access is sought on behalf of a  
4   client; and

5           causing a server operatively coupled to the client to request access to the  
6   target service on behalf of the client, from a trusted third party, wherein the  
7   server provides the trusted third party with a service credential authenticating  
8   the server, information about the target service, and a service credential  
9   previously provided by the client for the service, and wherein the service  
10   credential previously provided by the client includes implementation-specific  
11   identity information constraining a scope of access delegated to the server; and

12           causing the trusted third-party to provide the server with a new service  
13   credential ~~granted in the name of the client rather than the server~~ such that the  
14   new service credential authorizes the server to access the target service within  
15   the scope of access specified in the implementation-specific identity  
16   information.

17  
18           13.   (Original)   The method as recited in Claim 12, wherein the  
19   implementation-specific identity information includes information selected  
20   from a group comprising privilege attribute certificate (PAC) information,  
21   security identifier information, Unix identifier information, Passport identifier  
22   information, certificate information.

23  
24           14.   (Original)   The method as recited in Claim 13, wherein the  
25   PAC information includes compound identity information.

1           15.   (Original)   The method as recited in Claim 13, wherein the  
2   PAC information includes access control restrictions for use as delegation  
3   constraints.

4  
5           16.   (Currently Amended)   A computer-readable medium having  
6   computer-executable instructions for performing tasks for constraining a scope  
7   of delegation by a client to a server, comprising:

8           in a server, determining a target service to which access is sought on  
9   behalf of a client coupled to the server;

10          requesting a new service credential from a trusted third-party by  
11   providing the trusted third-party with a credential authenticating the server,  
12   information about the target service, and a service credential associated with  
13   the client and the requesting server such that issuance of the new service  
14   credential authorizes the server to access the service on behalf of the client  
15   while within a scope of delegation authorized by the client.

16  
17          17.   (Original)   The computer-readable medium as recited in Claim  
18   16, wherein the trusted third-party includes at least one service selected from a  
19   group of services comprising a key distribution center (KDC) service, a  
20   certificate granting authority service, and a domain controller service.

21  
22          18.   (Canceled).

1           19. (Previously Presented) The computer-readable medium as  
2 recited in Claim 16, wherein the service credential is configured for use by the  
3 server and the target service.  
4

5           20. (Previously Presented) The computer-readable medium as  
6 recited in Claim 16, wherein the credential authenticating the server includes a  
7 ticket granting ticket associated with the server.  
8

9           21. (Original) The computer-readable medium as recited in Claim  
10 16, further comprising:  
11

12           causing the trusted third-party to verify that the client has authorized  
13 delegation.  
14

15           22. (Original) The computer-readable medium as recited in Claim  
16 21, wherein:  
17

18           the trusted third-party includes a key distribution center (KDC); and  
19

20           causing the trusted third-party to verify that the client has authorized  
21 delegation includes verifying the status of a forwardable flag value as set by  
22 the client.  
23

24           23. (Original) The computer-readable medium as recited in Claim  
25 16, wherein the server is a front-end server with respect to a back-end server  
coupled to the front-end server, and wherein the back-end server is configured  
to provide the target service.

1           24. (Currently Amended) The computer-readable medium as  
2 recited in Claim 16, wherein:

3           the trusted third-party includes a key distribution center (KDC);

4           the KDC provides to the client authentication credentials of the client as  
5 a ticket-granting-ticket associated with the client ~~to the client~~; and

6           the client does not provide the ticket granting ticket to the server.

7  
8           25. (Original) The computer-readable medium as recited in  
9 Claim 16, wherein:

10          the trusted third-party includes a key distribution center (KDC); and

11          the requesting server requests the new service credential in a ticket  
12 granting service request message that includes a service ticket provided by the  
13 client to the server.

14  
15          26. (Currently Amended) A system comprising:

16          a credential granting mechanism configured to receive a request for a  
17 new service credential from a server and in response generate the new service  
18 credential granted in the name of a client rather than the server if delegation is  
19 allowable, and wherein the request includes:

20           a credential authenticating the requesting server,

21           identifying information about a target service to which access is sought  
22 on behalf of the client coupled to the server, and

23           a service credential that was previously granted to the client for use with  
24 the server and presenting a forwardable delegation flag indicating the client has  
25 authorized the delegation within a scope delegated by the client.

1           27. (Original) The system as recited in Claim 26, wherein the  
2 credential granting mechanism is provided by a trusted third party and includes  
3 at least one service selected from a group of services comprising a key  
4 distribution center (KDC) service, a certificate granting authority service, and a  
5 domain controller service.

6  
7           28. (Canceled).

8  
9           29. (Previously Presented) The system as recited in Claim 26,  
10 wherein the service credential is configured for use by the server and the target  
11 service.

12  
13           30. (Previously Presented) The system as recited in Claim 26,  
14 wherein the credential authenticating the server includes a ticket granting ticket  
15 associated with the server, and which was previously granted by the credential  
16 granting mechanism.



1           31. (Currently Amended) A system for constraining the scope of  
2 delegation by a client to a server, comprising:

3           a server configured to generate a request for a new service credential in  
4 the name of a client rather than the server from a trusted third-party, the new  
5 service credential being associated with a client and a target service, the  
6 request comprising:

7           a credential authenticating the server,  
8 information about the target service, and

9           a service credential associated with the client and the server wherein  
10 the server is constrained to access the target service within a scope specified by  
11 the client.

12  
13           32. (Original) The system as recited in Claim 31, wherein the  
14 trusted third-party includes at least one service selected from a group of  
15 services comprising a key distribution center (KDC) service, a certificate  
16 granting authority service, and a domain controller service.

17  
18           33. (Original) The system as recited in Claim 31, wherein the  
19 credential authenticating the server includes a ticket granting ticket associated  
20 with the server.

21  
22           34. (Original) The system as recited in Claim 31, wherein the  
23 server is a front-end server with respect to the service.  
24  
25

1           35. (Original) The system as recited in Claim 31, wherein the  
2 server requests the new service credential in a ticket granting service request  
3 message that includes the service ticket associated with the client and the  
4 server.

5  
6           36. (Withdrawn) A computer-readable medium having stored  
7 thereon a data structure, comprising:

8           a credential authenticating a first server,  
9           information identifying a second server, and  
10          a service credential associated with a client and the first server.

11  
12          37. (Withdrawn) The computer-readable medium as recited in Claim  
13 36, wherein the credential authenticating the first server includes a ticket-  
14 granting-ticket (TGT) and the service credential includes a service ticket.

15  
16          38. (Currently Amended) A method comprising:  
17          separately authenticating a server and a client;  
18          providing the server with a server ticket granting ticket;  
19          providing the client with a client ticket granting ticket and a service  
20 ticket for use with the server;

21          providing the server with a new service ticket in an identity of the client  
22 rather than an identity of the server for use by the server ~~for use with a new~~  
23 service while withholding from the server without requiring the server to have  
24 access to the client ticket granting ticket thereby constraining delegation of the  
25 client ticket granting ticket.

1           39. (Original) The method as recited in Claim 38, further  
2 comprising:

3           causing the server to request the new service ticket on behalf of the  
4 client by forwarding the server ticket granting ticket, information identifying  
5 the new service, and the service ticket to a trusted third party.  
6

7           40. (Currently Amended) A method for constraining a scope of  
8 delegation by a client to a server, comprising:

9           identifying a target service to which access is sought on behalf of a  
10 client that has been authenticated using a first authentication method;

11           causing a server that is operatively coupled to the target service and the  
12 client to request a service credential to itself from a second authentication  
13 method trusted third-party by identifying the client and the first authentication  
14 ~~protocol~~ method; and

15           causing the server to request from the second authentication method  
16 trusted third-party, a new service credential in an identity of the client rather  
17 than an identity of the server, for use by the server and the target service, ~~from~~  
18 ~~the second authentication method trusted third-party~~, wherein the server  
19 provides the trusted third-party with a credential authenticating the server to  
20 access the target service within a scope constrained by the client, information  
21 about the target service, and the service credential to itself.  
22  
23  
24  
25

1           41. (Original) The method as recited in Claim 40, wherein the  
2 second authentication method trusted third-party includes at least one service  
3 selected from a group of services comprising a key distribution center (KDC)  
4 service, a certificate granting authority service, and a domain controller  
5 service.

6  
7           42. (Canceled).

8  
9           43. (Previously Presented) The method as recited in Claim 40,  
10 wherein the service credential is configured for use by the server and the target  
11 service to which access is sought.

12  
13           44. (Previously Presented) The method as recited in Claim 40,  
14 wherein the credential authenticating the server includes a ticket granting ticket  
15 associated with the server.

16  
17           45. (Original) The method as recited in Claim 40, further  
18 comprising:

19           upon receiving a request for the new service credential from the server,  
20 causing the second authentication method trusted third-party to verify that the  
21 client has authorized delegation.

1           46. (Original) The method as recited in Claim 40, wherein the  
2 server is a front-end server with respect to a back-end server that is coupled to  
3 the front-end server, and wherein the back-end server is configured to provide  
4 the target service.

5  
6           47. (Original) The method as recited in Claim 40, wherein the  
7 first authentication method is selected from a group of authentication methods  
8 comprising Passport, SSL, NTLM, and Digest.

9  
10          48. (Original) The method as recited in Claim 40, wherein the  
11 second authentication method includes a Kerberos authentication protocol.  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

1           49. (Currently Amended) A computer-readable medium having  
2 computer-executable instructions for performing tasks for constraining a scope  
3 of delegation by a client to a server, comprising:

4           identifying a target service to which access is sought on behalf of a  
5 client that has been authenticated using a first authentication method;

6           causing a server that is operatively coupled to the target service and the  
7 client to request a service ticket to itself from a second authentication method  
8 trusted third-party by identifying the client and the first authentication method  
9 protocol; and

10           causing the server to request a new service ticket in an identity of the  
11 client rather than an identity of the server, for use by the server and the  
12 identified service, from the second authentication method trusted third-party,  
13 wherein the server provides the trusted third-party with a ticket authenticating  
14 the server to act within a scope of delegation permitted by the client,  
15 information about the target service, and the service ticket to itself.

16  
17           50. (Original) The computer-readable medium as recited in Claim  
18 49, wherein the second authentication method trusted third-party includes a  
19 key distribution center (KDC).

20  
21           51. (Canceled).

22  
23           52. (Previously Presented) The computer-readable medium as  
24 recited in Claim 49, wherein the service ticket is configured for use by the  
25 server and the target service.

1           53. (Previously Presented) The computer-readable medium as  
2 recited in Claim 49, wherein the ticket authenticating the server includes a  
3 ticket granting ticket associated with the server.

4  
5           54. (Original) The computer-readable medium as recited in Claim  
6 49, further comprising:

7           upon receiving a request for the new service ticket from the server,  
8 causing the second authentication method trusted third-party to verify that the  
9 client has authorized delegation.

10  
11           55. (Original) The computer-readable medium as recited in Claim  
12 49, wherein the server is a front-end server with respect to a back-end server  
13 that is coupled to the front-end server, and wherein the back-end server is  
14 configured to provide the target service.

15  
16           56. (Original) The computer-readable medium as recited in Claim  
17 49, wherein the first authentication method is selected from a group of  
18 authentication methods comprising Passport, SSL, NTLM, and Digest.

19  
20           57. (Original) The computer-readable medium as recited in Claim  
21 49, wherein the second authentication method includes a Kerberos  
22 authentication protocol.

1           58. (Currently Amended) A system for constraining a scope of  
2 delegation by a client to a server, comprising:

3           a server configurable to:

4           identify a target service to which access is sought on behalf of a  
5 client that has been authenticated using a first authentication method,

6           request a service credential to itself from a second authentication  
7 method trusted third-party by identifying the client and the first  
8 authentication method, and

9           subsequently request a new service credential, for use by the server  
10 and the target service, from the second authentication method trusted third-  
11 party,

12           wherein the server provides the second authentication method  
13 trusted third-party with a credential authenticating the server, information  
14 about the target service, and the service credential to itself in an identity of  
15 the client rather than the server such that a scope of delegation authorized  
16 by the client constrains access by the server to the target service as  
17 authorized by the client.

18  
19           59. (Canceled).

20  
21           60. (Previously Presented) The system as recited in Claim 58,  
22 wherein the new service credential is configured for use by the server and the  
23 target service.  
24  
25



1           61. (Previously Presented) The system as recited in Claim 58,  
2 wherein the credential authenticating the server includes a ticket granting ticket  
3 associated with the server.  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25